REMARKS

Applicant appreciates the time taken by the Examiner to review Applicant's present application. This application has been carefully reviewed in light of the Official Action mailed May 9, 2006.

Rejections under 35 U.S.C. § 103

Claims 1, 3-5, 7, 13, 14, 17, 22, 25 and 29 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Publication No. 2002/0068629 ("Allen") in view of U.S. Patent No. 6,968,364 ("Wong").

In order to establish a prima facie case of obviousness, the Examiner must show: that the prior art references teach or suggest all of the claim limitations; that there is some suggestion or motivation in the references (or within the knowledge of one of ordinary skill in the art) to modify or combine the references; and that there is a reasonable expectation of success. M.P.E.P. 2142, 2143; In re Vaeck, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991). The Examiner must explain with reasonable specificity at least one rejection – otherwise, the Examiner has failed procedurally to establish a prima facie case of obviousess. M.P.E.P. 2142; Ex parte Blanc, 13 U.S.P.Q.2d 1383 (Bd. Pat Application. & Inter. 1989). When the motivation to combine the teachings of the references is not immediately apparent, it is the duty of the Examiner to explain why the combination of the teachings is proper. Ex parte Skinner, 2 U.S.P.Q.2d 1788, 1790 (Bd. Pat. App. & Inter. 1986).

Claim 1 recites:

> A method of conducting a secure transaction with an on-line service while offline comprising the steps of:
>
> issuing a transaction authorization token to a user from an application server for the on-line service while the user is online with the on-line service;
>
> preparing an off-line transaction object containing data to specify and request the secure transaction;
>
> sending a message to the on-line service, said message containing the off-line transaction object and the transaction authorization token;
>
> upon receipt of said message, the application server validating the transaction authorization token to authenticate the user and to authorize the secure transaction, wherein the application server performs said validating while the user is offline from the on-line service; and

executing the off-line transaction object if the secure transaction is authorized. [Emphasis Added]

According to Claim 1, an application server issues a transaction authorization token to a user. The user, while off-line with the online service, can then prepare an off-line transaction object and send a message to the on-line service containing the off-line transaction object and the transaction authorization token. The application server validates the transaction authorization token to authenticate the user and authorize the transaction requested in the transaction object. The application server performs the validating while the user is offline from the on-line service. Thus, the authorization token issued by the online service is later used by the on-line service to authenticate the user and authorize a transaction requested in the transaction object while the user is offline from the on-line service. Claim 29 includes similar features.

Applicant respectfully submits that neither Allen nor Wong teach or suggest i) the application server validating the transaction authorization token to authenticate the user and to authorize the secure transaction or ii) the application server performing the validating while the user is off-line from the online service. Allen teaches a system in which the user must authenticate with a gaming server before providing a gaming token to the gaming server. Consequently, the gaming server does not validate the token to authenticate the user or validate the token while the user is offline. Wong teaches a system in which a token is sent to a personal video recorder ("PVR") and processed at the PVR to determine which shows to record. The token is not sent back to the application server of Wong. Again, the server of Wong that provides the token does not validate the token to authenticate the user while the user is offline with the server.

Allen

Allen does not teach or suggest that the application server validates the token to authenticate the user and to authorize the secure transaction while the user is off-line with online service. Instead, Allen teaches a system in which a user obtains a gaming token having a monetary value, which allows a user to a play a game and change the value of the token while the user is off-line. *See* Allen ¶0008. The gaming token contains various fields that ensure the value of the gaming token is only modified in permitted manners. *See* Allen ¶0033, 0052. In order to redeem the gaming token, the user reestablishes a network connection with

the gaming service. *See* Allen ¶0050. This can be done by submission of a valid password and user ID from the client computer. *See* Allen ¶0050. If an active account exists for the user, the client uploads the gaming token. *See* Allen ¶0051. The gaming provider server then takes steps to "determine the authentication of the token 246 at step 612" (emphasis added). *See* Allen ¶0052. This authentication involves determining whether the token has been corrupted accidentally or intentionally. *See* Allen ¶0052. If the token is authenticated, the gaming service provider credits the user's account. *See* Allen ¶0053.

The system of Allen provides an example of a traditional system with limitations that the present invention seeks to overcome. Specifically, the system of Allen requires the user to authenticate at log-in by entering a password or otherwise presenting credentials established as a consequence of the user being on a network and requires the user to be on-line at the point in time when the transaction is authorized. *See* '401 Application, page 2, lines 1-10 (discussing traditional web-based financial transactions) and Allen ¶¶0050-51 (discussing that a user must log-on to the gaming provider and authenticate with the gaming provider before uploading the gaming token). While the system of Allen does determine the authentication of the token to determine if the token has been corrupted, the system of Allen does not use the token itself to authenticate the user. Thus, the gaming provider server of Allen does not perform the step of "validating the token to authenticate the user and authorize the secure transaction." Moreover, in Allen, the step of determining the authentication of the token occurs while the user is online with the gaming provider server. Therefore, the validating of the token does not occur while the user is off-line with the gaming service.

Wong

Before addressing the teachings of Wong, Applicant notes that a prior art reference must be considered for everything it teaches. In this regard, "it is impermissible within the framework of section 13 to pick and choose from any one reference only so much of it as will support a given position to the exclusion of other parts necessary to the full appreciation of of what such reference fairly suggests to one of ordinary skill in the art." *In re Wesslau,* 353 F.2d 238, 241, 147 U.S.P.Q. 391, 393 (C.C.P.A) 1965, *see also Bausch & Lomb, Inc. v. Barnes-Hind/Htydrocurve, Inc.,* 796 F.2d 443, 448-49, 230 U.S.P.Q. 416, 420 (Fed. Cir. 1986).

Wong teaches a system for programming personal video recorders ("PVR") such as digital video recorders ("DVR") to record specified programs. According to Wong, a user may

access a server to select one or more programs to record. *See* Wong, col. 6, lines 58-57. Program information identifying one or more selected programs can be sent to the client computer or to another recipient as a token. *See* Wong, col. 14, lines 51-62. The tokens can be used at the client computer to cause an associated PVR or a remote PVR to record the audio and/or visual broadcast programming identified by the token. *See* Wong, col. 19, lines 61-64. As described in Wong:

> When email reader 400 is part of a remote computer, the RECORD button 424 may cause the token to be sent as part of an email message to an email address of the user's (or another person's) PVR. As mentioned above, a PVR may be programmed to automatically program operation of the PVR in response to receiving an email message having a token from a pre-authorized source. The authorization or authentication, for example, may be determined based on the email address of the sender, a password provided with the email (e.g., as part of the token or another attachment), or another authorization technique.

See Wong, col. 20, lines 4-14 (emphasis added). In this case, it is the recipient of the token (i.e, the PVR that will record the program) that authenticates the token to determine if it is from an authorized source. The server that issues the token to the client computer does not receive the token back from the DVR (or client computer) and validate the token to authenticate the user and authorize the transaction. Consequently, Wong does not teach or suggest that the application server validate the token while the user is offline with the on-line service.

In addressing authentication at the online service, Wong only teaches that a user must be online with the online service to authenticate (i.e., by logging onto the online service through a web page). Specifically, a user provides identifying data "when a user logs into a service, such as a web site." *See* Wong, col. 24, line 63 through col. 25, line 16 and FIGURES 10a-11 (discussing user authentication with a service to illustrating a link to log-in to the service). Thus, secure communications with the service occur when the user is on-line with the on-line service. There is no teaching that a user is authenticated with the application server of the online service using a token while off-line with the online service.

Combination of Wong and Allen

The Examiner stated that "it would have been obvious to one of ordinary skill in the art at the time the invention was made, to combine the transaction authorization token, sending the transaction authorization token in a message, and validating the transaction authorization token while the user is off-line, as taught by Wong et al., with the method of Allen et al. It would have been obvious for such modification because a transaction token allows automatic configuration of the PVR, or any other device, in response to receiving a message containing the transaction authorization token (*see* col. 20, lines 7-14 of Wong et al.)." Applicant respectfully submits that the Examiner has stated a feature of Wong (i.e., the ability to configure a PVR in response to receiving a message containing a token) without actually providing any reason why one would be motivated to include this feature in the method of Allen. Under the Examiner's stated reasoning, the mere fact that Wong teaches a particular function is motivation enough to use that feature in any system. The mere fact that a feature is known from one reference is not sufficient to motivate one to combine that reference with another. The Examiner has not pointed to any teaching in the art that suggests the desirability or incentive to make the modification needed to arrive at the claimed invention.

Moreover, even if combined, Allen and Wong do not teach or suggest the present invention as recited in Claim 1 and Claim 29 because neither Alan nor Wong teach or suggest that the application server for the online service uses the transaction authentication token to authenticate the user while the user is off-line with the online service. Alan and Wong both teach that the user is online with the service and authenticates with the server using a user name and password or otherwise presenting credentials established as a consequence of being on the network. Thus, even if combined, Alan and Wong would suggest that the user must be on-line with the application server to authenticate with the application server of the on-line service.

New Claims 30-32

New Claim 30 recites that the transaction object includes an instruction to execute a function. Thus, the transaction object requests a particular function or functions by the on-line service and is not simply a set of data utilized by the on-line service in performing a function. This is supported by the specification at page 8, lines 7-8, which states "a transaction object is a

command, instruction, query or the like to execute an authorized function, together with the data required to execute the function."

New Claim 31 recites that "the authorization token is a separate object from the off-line transaction object." This is supported at various places in the specification. For example, page 9, lines 1-16 describe an application first checking a transaction token for validity and then checking the transaction object for conformity with the token. Additionally, page 8, lines 4-7 describe a "security access token" as a file, a certificate, a character string or the like that encodes an authorization for a specified type of transaction by the specific user over a specified set of data objects and as a data object that is used for authorizing access to an transactions on the application.

Thus, according to Claim 31, which depends from Claim 1, the transaction authorization token used to authenticate the user and authorize a requested transaction is separate from the transaction object that contains the data to specify and request the transaction.

Conclusion

Applicant appreciates the time taken by the Examiner to review the present application. For the foregoing reasons, Applicant respectfully submits that Claims 1 and 29 are allowable over Allen and Wong. Therefore, Applicant respectfully requests allowance of these claims and the respective dependent Claims. Additionally, Applicant respectfully requests allowance of Claims 30 and 31.

Applicant has now made an earnest attempt to place this case in condition for allowance. Other than as explicitly set forth above, this reply does not include an acquiescence to statements, assertions, assumptions, conclusions, or any combination thereof in the Office Action. For the foregoing reasons and for other reasons clearly apparent, Applicant respectfully requests full allowance of Claims 1-31. The Examiner is invited to telephone the undersigned at the number listed below for prompt action in the event any issues remain.

The Director of the U.S. Patent and Trademark Office is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 50-3183 of Sprinkle IP Law Group.

Respectfully submitted,

Sprinkle IP Law Group
Attorneys for Applicant

John L. Adair
Reg. No. 48,828

Date: August 9, 2006

1301 W. 25th Street, Suite 408
Austin, TX 78705
Tel. (512) 637-9220
Fax. (512) 371-9088